DERWENT-ACC-NO: 2001-202471

DERWENT-WEEK: 200645

COPYRIGHT 2007 DERWENT INFORMATION LTD

TITLE: Access security of data in a portable mass memory to protect against copying uses scrambled data

INVENTOR: NEIFER, W

PATENT-ASSIGNEE: SCM MICROSYSTEMS GMBH[SCMMN]

PRIORITY-DATA: 1999DE-1012224 (March 18, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
DE 50012858 G	July 6, 2006	N/A	000	G06F 001/00
WO 200055707 A1	September 21, 2000	G	021	G06F 001/00
EP 1161717 A1	December 12, 2001	G	000	G06F 001/00
JP 2002539551 W	November 19, 2002	N/A	022	G06F 012/14
EP 1161717 B1	May 31, 2006	G	000	G06F 001/00

DESIGNATED-STATES: JP SG US AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
DE 50012858G	N/A	2000DE-0512858	March 17, 2000
DE 50012858G	N/A	2000EP-0926741	March 17, 2000
DE 50012858G	N/A	2000WO-EP02414	March 17, 2000

DE 50012858G	Based on	EP 1161717	N/A
DE 50012858G	Based on	WO 200055707	N/A
WO 200055707A1	N/A	2000WO-EP02414	March 17, 2000
EP 1161717A1	N/A	2000EP-0926741	March 17, 2000
EP 1161717A1	N/A	2000WO-EP02414	March 17, 2000
EP 1161717A1	Based on	WO 200055707	N/A
JP2002539551W	N/A	2000JP-0605871	March 17, 2000
JP2002539551W	N/A	2000WO-EP02414	March 17, 2000
JP2002539551W	Based on	WO 200055707	N/A
EP 1161717B1	N/A	2000EP-0926741	March 17, 2000
EP 1161717B1	N/A	2000WO-EP02414	March 17, 2000
EP 1161717B1	Based on	WO 200055707	N/A

INT-CL (IPC): G06F001/00, G06F003/06 , G06F012/14 , G11B020/00

ABSTRACTED-PUB-NO: WO 200055707A

BASIC-ABSTRACT:

NOVELTY - Multi media information and software is stored in a portable mass memory module (22) and this contains data in distorted form. It may only be descrambled by entry of a personal identification when it is plugged into the processing system (10). The authorization code is also stored in a personal series analogue memory,SAM, in the module and must be matched with the entered code.

USE - Commercial software protection

ADVANTAGE - Protects against illegal copying

DESCRIPTION OF DRAWING(S) - Block diagram

Memory module 22

Processing system 10

CHOSEN-DRAWING: Dwg.1/4

TITLE-TERMS: ACCESS SECURE DATA PORTABLE MASS MEMORY PROTECT COPY SCRAMBLE DATA

DERWENT-CLASS: S05 T01 T05

EPI-CODES: S05-D01C5A; T01-H01C2; T01-J12C; T05-D01B;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2001-144473

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation [7]: G06F 1/00, G11B 20/00	A1	(11) Internationale Veröffentlichungsnummer: WO 00/55707
		(43) Internationales Veröffentlichungsdatum: 21. September 2000 (21.09.00)

(21) Internationales Aktenzeichen: PCT/EP00/02414

(22) Internationales Anmeldedatum: 17. März 2000 (17.03.00)

(30) Prioritätsdaten:
199 12 224.5 18. März 1999 (18.03.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, D-85276 Pfaffenhofen (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: NEIFER, Wolfgang [DE/DE]; Rosenstrasse 9a, D-85354 Freising (DE).

(74) Anwalt: DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, D-81241 München (DE).

(81) Bestimmungsstaaten: JP, SG, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

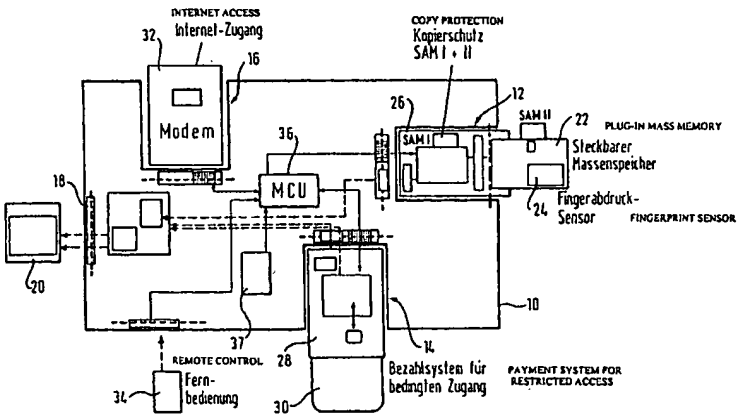
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD OF SECURING DATA IN A PORTABLE MASS MEMORY AGAINST UNAUTHORIZED DUPLICATION

(54) Bezeichnung: VERFAHREN ZUR SICHERUNG VON DATEN IN EINEM TRAGBAREN MASSENSPEICHER GEGEN UNAUTORISIERTE VERVIELFÄLTIGUNG

(57) Abstract

To secure multimedia information and software stored in a portable mass memory (22) against unauthorized duplication the data are stored in said mass memory (22) in distorted form. In the system (10) for playing back the data a personal identity code of the authorized user is stored in a personal serial analog memory (SAM) module. The correction keys necessary for correction of the data are stored in the SAM module of the authorized user. An authorization code is assigned to said data, which is also stored in the SAM module. An authorization code encoded by means of the personal identity code is generated in the SAM module and then stored in the mass memory (22). Before the data are played back the encoded authorization code is decoded by the SAM module by means of the personal identity code. The decoded authorization code is then compared with the authorization code stored in the SAM module and correction by means of the correction key of the data read out from the mass memory (22) is approved only if the authorization codes coincide.



(57) Zusammenfassung

Zur Sicherung von multimedialen Informationen und Software in einem tragbaren Massenspeicher (22) gegen unautorisierte Vervielfältigung werden die Daten in dem Massenspeicher (22) in verzerrter Form gespeichert. In dem Wiedergabesystem (10) für die Daten wird auf einem persönlichen SAM–Modul ein persönlicher Identitätscode des autorisierten Benutzers gespeichert. Die zur Entzerrung der Daten benötigten Entzerrungs–Schlüssel werden auf den SAM–Modul des autorisierten Benutzers gespeichert. Den Daten wird ein Autorisierungs–Code zugeordnet, der auf dem SAM–Modul abgelegt wird. Auf dem SAM–Modul wird ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet und dann auf dem Massenspeicher (22) abgelegt. Vor der Wiedergabe der Daten wird der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscodes vom SAM–Modul entschlüsselt. Der entschlüsselte Autorisierungscode wird mit dem auf dem SAM–Modul abgelegten Autorisierungscode verglichen. Die Entzerrung der vom Massenspeicher (22) ausgelesenen Daten mittels des Entzerrungsschlüssels wird nur bei übereinstimmenden Autorisierungscodes freigegeben.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung

Die Erfindung betrifft ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung und ein Wiedergabesystem zur Durchführung des Verfahrens.

Die kommerzielle Verbreitung von multimedialen Inhalten und Software geschieht ganz überwiegend auf Datenträgern, die nur einmal beschreibbar sind und mit dem darauf gespeicherten Inhalt das Handelsprodukt bilden. Die kommerzielle Verbreitung der Inhalte losgelöst von solchen Datenträgern wäre prinzipiell möglich, beispielsweise durch Fernzugriff auf Netzwerke mit Bezahlfunktion, scheitert jedoch am mangelnden Schutz gegen unautorisierte Vervielfältigung.

Durch die Erfindung wird ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung zur Verfügung gestellt, das mit geringem Aufwand und verfügbarer Technologie durchgeführt werden kann. Nach dem erfindungsgemäßen Verfahren werden die Daten in dem Massenspeicher zunächst in verzerrter Form gespeichert. In einem Wiedergabesystem für die Daten wird wenigstens ein SAM-Modul (Safe Access Modul, d.h. Modul für gesicherten Zugriff) verwendet, auf dem ein persönlicher Identitätscode eines autorisierten Benutzers gespeichert ist. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf dem SAM-Modul des autorisierten Benutzers gespeichert. Den Daten wird ein Autorisierungscode zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul wird sodann ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet. Dieser verschlüsselte Autorisierungscode wird mit den verzerrten Daten auf dem Massenspeicher abgelegt. Vor einer Wiedergabe der Daten wird der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscode vom SAM-Modul entschlüsselt. Der entschlüsselte Autorisierungscode wird dann mit dem auf dem SAM-Modul (unverschlüsselt) abgelegten Autorisierungscode verglichen. Die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels der Entzerrungsschlüssel wird dann nur bei übereinstimmenden

Autorisierungscodes freigegeben. Durch dieses mit einfachster Hardware durchführbare Verfahren erfolgt eine Personalisierung der Daten auf dem Massenspeicher. Für die unverzerrte Wiedergabe der Daten wird ein Autorisierungscode benötigt, der nur über den SAM-Modul des autorisierten Benutzers gewonnen werden kann, weil er mit dem persönlichen Identitätscode des autorisierten Benutzers verknüpft ist.

In Weiterbildung des Verfahrens werden auch die für die Entzerrung der Daten benötigten Entzerrungsschlüssel mit auf dem SAM-Modul gespeicherten persönlichen Daten des autorisierten Benutzers chiffriert, so daß sie nur unter Verwendung des zutreffenden SAM-Moduls dechiffriert werden können.

In weiterer Ausgestaltung des Verfahrens werden die Daten bei der Wiedergabe über ein geeignetes Wiedergabesystem unlösbar mit einer persönlichen Kennzeichnung des autorisierten Benutzers ausgegeben. Die persönliche Kennzeichnung kann in einem Logo oder dergleichen bestehen, das bei Bilddaten in einer Ecke des Bildfeldes angezeigt wird.

Das erfindungsgemäße Wiedergabesystem zur Durchführung des Verfahrens enthält im wesentlichen: Ein Lesemodul zur Aufnahme des Massenspeichers, bei dem es sich vorzugsweise um ein vom Anwender beschreibbares Medium handelt, beispielsweise eine miniaturisierte Festplatte oder eine vom Benutzer beschreibbare optische Speicherplatte; einen Kartenleser für das SAM-Modul; eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und ein Ausgabegerät für die entzerrten Daten. Um Daten über ein entferntes Netzwerk, beispielsweise aus dem Internet, beziehen zu können, ist vorzugsweise zusätzlich ein Bezahlsystem für den bedingten Zugang zu einem Datenanbieter über das entfernte Netzwerk vorgesehen. Das Bezahlsystem basiert auf einem Chipkartenleser, der bei der bevorzugten Ausführungsform als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus der folgenden Beschreibung und aus der Zeichnung, auf die Bezug genommen wird. In der Zeichnung zeigen:

Das in Figur 1 gezeigte Blockschaltbild eines Wiedergabesystems zur Durchführung des erfindungsgemäßen Verfahrens zeigt schematisch die wesentlichen Komponenten des Systems. Eine in einem kompakten Gehäuse untergebrachte Schnittstelleneinrichtung ist allgemein mit 10 bezeichnet und weist drei Schnittstellen 12, 14, 16 für steckbare Komponenten sowie einen Ausgangsanschluß 18 für ein Video-Ausgabegerät 20 auf. Die Schnittstelle 12 hat einen Stecksockel für einen Massenspeicher 22, der auf einer dem Benutzer zugänglichen Fläche einen Fingerabdruck-Sensor 24 aufweist. Ein erstes SAM-Modul 26 ist Bestandteil der Schnittstelle 12. Ein zweites SAM-Modul ist in dem steckbaren Massenspeicher 22 enthalten. Dieser Massenspeicher kann eine miniaturisierte Festplatte oder auch ein Halbleiterspeicher sein, beispielsweise in FLASH-Techologie.

Die Schnittstelle 14 nimmt einen Chipkartenleser 28 im Format einer PC-Karte (Abkürzung für PCMCIA-Karte) auf. Der Chipkartenleser 28 bildet in Verbindung mit einer Chipkarte 30, auch als Smart Card bezeichnet, ein Bezahlsystem für den bedingten Zugang zu einem Anbieter multimedialer Inhalte und dergleichen, insbesondere über das Internet.

An der Schnittstelle 16 wird ein Modem 32 oder ein Netzwerkadapter angeschlossen. Über das Modem 32 oder den Netzwerkadapter kann der Zugriff auf ein entferntes Netzwerk, insbesondere das Internet, erfolgen.

Am Ausgangsanschluß 18, der als SCART-Schnittstelle ausgeführt sein kann, wird ein Fernsehempfänger oder Monitor angeschlossen.

Das Wiedergabesystem kann ferner mit einer Infrarot-Fernbedienung 34 ausgestattet sein.

Ein interner Prozessor 36 beinhaltet die notwendige Funktionalität zur Entzerrung und Aufbereitung der von dem Massenspeicher 22 ausgelesenen Daten für die Wiedergabe auf dem Ausgabegerät 20. Der Prozessor 36 ist mit einem synchronisierten Zeitgeber 37 gekoppelt, der Bestandteil einer Überwachungseinrichtung ist, mittels welcher die Aufbereitung der Daten zur Wiedergabe von einem zertifizierten Zeitstempel abhängig gemacht wird, der mit den Daten auf dem Massenspeicher 22 aufgezeichnet ist.

Das erfindungsgemäße Verfahren ist in den Diagrammen der Figuren 2, 3 und 4 dargestellt. Es besteht im wesentlichen aus drei Stufen. In der ersten, in Figur 2 dargestellten Stufe des Verfahrens erfolgt eine Personalisierung der Daten im Massenspeicher. Der Vorgang wird mit der Übersendung eines System-Zertifikats zum Anbieter der Daten begonnen. Bei den Daten handelt es sich insbesondere um multimediale Informationen, abgekürzt als MMI. Durch das Systemzertifikat weist sich das Wiedergabesystem beim MMI-Anbieter als geeignetes System aus. Seitens des MMI-Anbieters wird dann aus dem SAM-Modul des Wiedergabesystems ein privater Schlüssel empfangen, um einen Wiedergabe-Autorisierungscode zu erzeugen. Bei dem privaten Schlüssel kann es sich um einen persönlichen Identitätscode oder auch um vom Fingerabdruck-Sensor 24 abgeleitete komprimierte Daten, oder eine Kombination derselben, handeln. Der Wiedergabe-Autorisierungscode wird dann auf dem SAM-Modul gespeichert.

Anschließend erfolgt mittels des Bezahlsystems 28, 30, die Bezahlung, woraufhin die MMI-Daten in verzerrter Form heruntergeladen und auf dem MMI-Massenspeicher 22 gespeichert werden. Anschließend werden die zur Entzerrung der MMI-Daten benötigten MMI-Schlüssel in chiffrierter Form zum SAM-Modul übertragen und dort gespeichert. Ferner wird vom MMI-Anbieter ein chiffriertes Wasserzeichen gesendet, das im SAM-Modul gespeichert werden kann, wenn der Umfang der entsprechenden Daten vergleichsweise gering ist; andernfalls erfolgt die Speicherung im Massenspeicher. Optional wird mit den MMI-Daten ein zertifizierter Zeitstempel gesendet und auf dem Massenspeicher 22 aufgezeichnet.

Als letzter Schritt der ersten Verfahrensstufe wird vom MMI-Anbieter ein chiffrierter Autorisierungscode gesendet, der im MMI-Massenspeicher zusammen mit den MMI-Daten gespeichert wird.

Wenn in den privaten Schlüssel die durch den Fingerabdruck-Sensor abgegebenen Daten eingehen, können diese durch den im Massenspeicher 22 integrierten SAM-Modul ver- oder bearbeitet werden.

Die in Figur 3 gezeigte Verfahrensstufe betrifft die Überprüfung der Wiedergabe-Autorisierung. In dem SAM-Modul wird dazu der aus dem Massenspeicher gelesene chiffrierte Autorisierungscode mittels des privaten Schlüssels dechiffriert; der so zurückgewonnene Autorisierungscode wird dann mit dem auf dem SAM-Modul gespeicherten Autorisierungscode verglichen. Bei übereinstimmenden Autorisierungscodes wird der Wiedergabeprozeß freigegeben.

Bei dem in Figur 4 gezeigten Wiedergabe-Prozeß wird zunächst im SAM-Modul der MMI-Schlüssel mittels des privaten Schlüssels dechiffriert. Dann werden die MMI-Daten aus dem Massenspeicher ausgelesen und mittels des dechiffrierten MMI-Schlüssels entzerrt. Die entzerrten MMI-Daten werden dann mit dem persönlichen Logo bzw. Wasserzeichen überlagert und an das Ausgabegerät abgegeben.

Durch den optional mit den MMI-Daten aufgezeichneten zertifizierten Zeitstempel kann die zugelassene Wiedergabe der Daten zeitlich befristet werden.

Patentansprüche

1. Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unautorisierte Vervielfältigung, insbesondere zum Schutz von multimedialen Informationen und Software, dadurch gekennzeichnet, daß:

a) die Daten in dem Massenspeicher in verzerrter Form gespeichert werden;

b) in einem Wiedergabesystem für die Daten wenigstens ein persönlicher SAM-Modul verwendet wird, auf dem ein persönlicher Identitätscode des autorisierten Benutzers gespeichert ist;

c) wenigstens ein zur Entzerrung der Daten benötigter Entzerrungsschlüssel auf dem SAM-Modul des autorisierten Benutzers gespeichert wird;

d) den Daten ein Autorisierungs-Code zugeordnet wird, der auf dem SAM-Modul abgelegt wird;

e) auf dem SAM-Modul ein mittels des persönlichen Identitätscodes verschlüsselter Autorisierungscode gebildet wird;

f) der verschlüsselte Autorisierungscode auf dem Massenspeicher abgelegt wird;

g) vor einer Wiedergabe der Daten der verschlüsselte Autorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul entschlüsselt wird;

h) der entschlüsselte Autorisierungscode mit dem auf dem SAM-Modul abgelegten Autorisierungscode verglichen wird und die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels des Entzerrungsschlüssels nur bei übereinstimmenden Autorisierungscodes freigegeben wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vor dem Erwerb der Daten von einem Anbieter ein System-Zertifikat vom SAM-Modul zum Anbieter gesendet und von diesem überprüft wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für die gesicherte Übertragung des Autorisierungscodes zum SAM-Modul des autorisierten Benutzers ein Sitzungsschlüssel verwendet wird.

4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zur Personalisierung der Daten auf dem Massenspeicher eine Kennzeichnung aus persönlichen Merkmalen des autorisierten Benutzers gebildet und mit den Daten in solcher Weise verknüpft wird, daß die Daten nur mit der Kennzeichnung ausgegeben werden können.

5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der persönliche Identitätscode des autorisierten Benutzers zumindest teilweise aus von einem Fingerabdruck-Sensor gelieferten Daten gebildet wird.

6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher in einem an einem Wiedergabesystem steckbaren Modul angeordnet ist.

7. Verfahren nach den Ansprüchen 5 und 6, dadurch gekennzeichnet, daß der Fingerabdruck-Sensor auf einer Fläche des steckbaren Moduls angeordnet ist.

8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß mittels eines ersten, im Wiedergabesystem angeordneten SAM-Moduls die Kommunikation und Transaktion mit dem Anbieter der Daten und mittels eines zweiten, dem Massenspeicher zugeordneten SAM-Moduls die Personalisierung der Daten abgewickelt werden.

9. Verfahren nach den Ansprüchen 6 und 8, dadurch gekennzeichnet, daß das dem Massenspeicher zugeordnete SAM-Modul in das steckbare Modul integriert ist.

10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher als miniaturisierte Festplatte ausgebildet ist.

11. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Massenspeicher als Flash-Halbleiterspeicher ausgebildet ist.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß der Flash-Halbleiterspeicher entfernbar in einem am Wiedergabesystem steckbaren Schnittstellen-Modul angeordnet ist.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß das Schnittstellen-Modul einen SAM-Kartenleser enthält.

14. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zum Erwerb der Daten eine Kommunikation und Transaktion mit einem Anbieter per Fernzugriff auf ein Netzwerk erfolgt.

15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß die Transaktion mit dem Anbieter unter Verwendung eines in das Wiedergabesystem einsteckbaren Kartenleser-Moduls erfolgt, das einen Chipkartenleser und einen das wenigstens eine SAM-Modul aufnehmenden SAM-Kartenleser beinhaltet.

16. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Entzerrungsschlüssel seinerseits mit auf dem SAM-Modul gespeicherten persönlichen Daten chiffriert und bei der Wiedergabe mit diesen Daten dechiffriert wird.

17. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß ein zertifizierter Zeitstempel erzeugt und mit den Daten auf dem Massenspeicher gespeichert wird.

18. Wiedergabesystem zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, gekennzeichnet durch:

- ein Lesemudul zur Aufnahme des Massenspeichers;
- einen Kartenleser für das SAM-Modul;
- eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und
- ein Ausgabegerät für die entzerrten Daten.

19. Wiedergabesystem nach Anspruch 16, ferner gekennzeichnet durch ein auf einem Chipkartenleser basierendes Bezahlsystem für bedingten Zugang zu einem Datenanbieter über ein entferntes Netzwerk.

20. Wiedergabesystem nach Anspruch 17, dadurch gekennzeichnet, daß der Chipkartenleser als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

21. Wiedergabesystem nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß eine Überwachungseinrichtung vorgesehen ist, die einen mit den Daten vom Massenspeicher gelesenen zertifizierten Zeitstempel auswertet.

Fig. 1

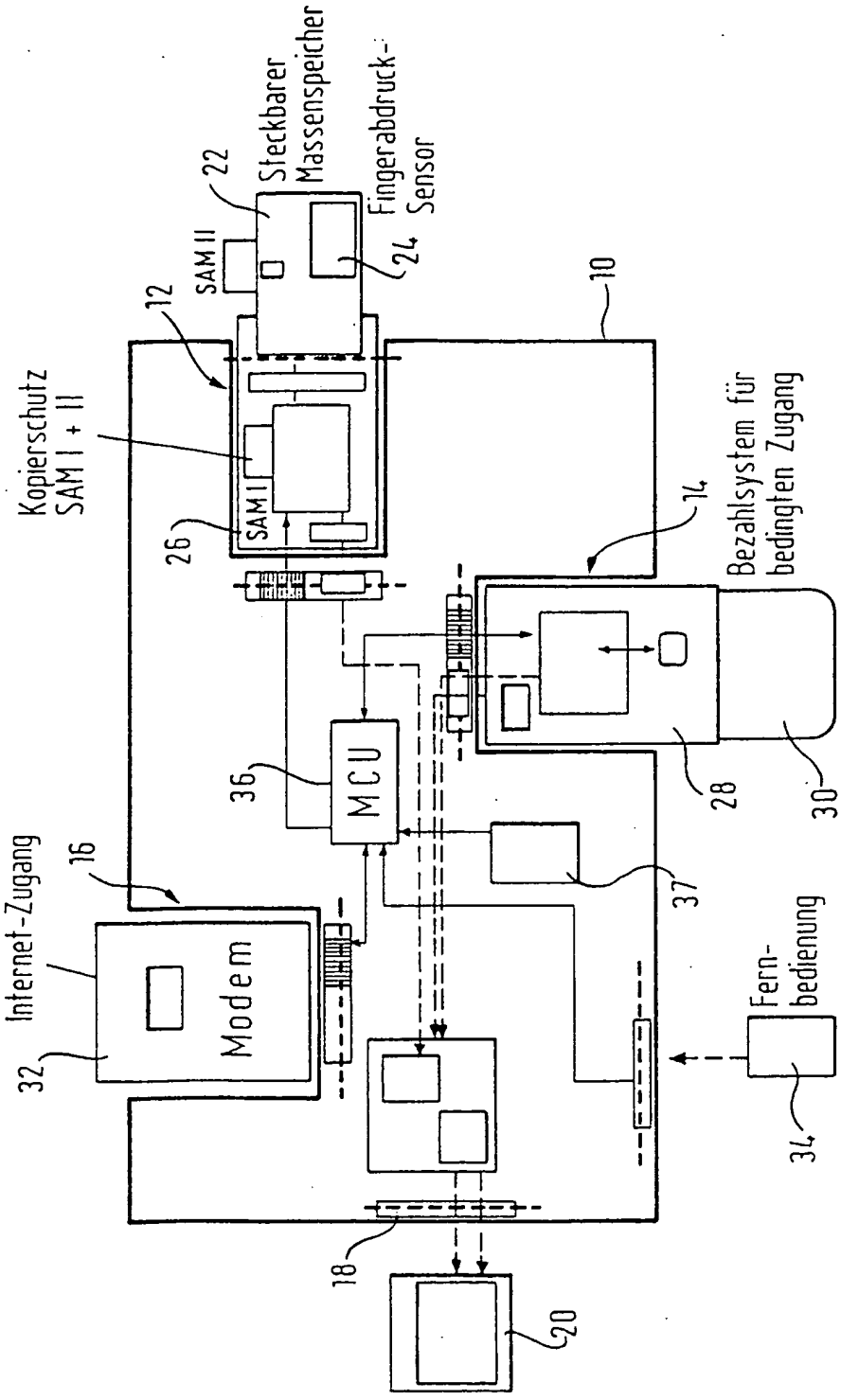

Steckbarer Massenspeicher
Fingerabdruck-Sensor
SAM II
22
24
12
10
Kopierschutz SAM I + II
SAM I
26
14
Bezahlsystem für bedingten Zugang
36
MCU
28
30
37
16
Internet-Zugang
Modem
32
Fern-bedienung
34
18
20

Fig. 2

Personalisierung MMI-Massenspeicher

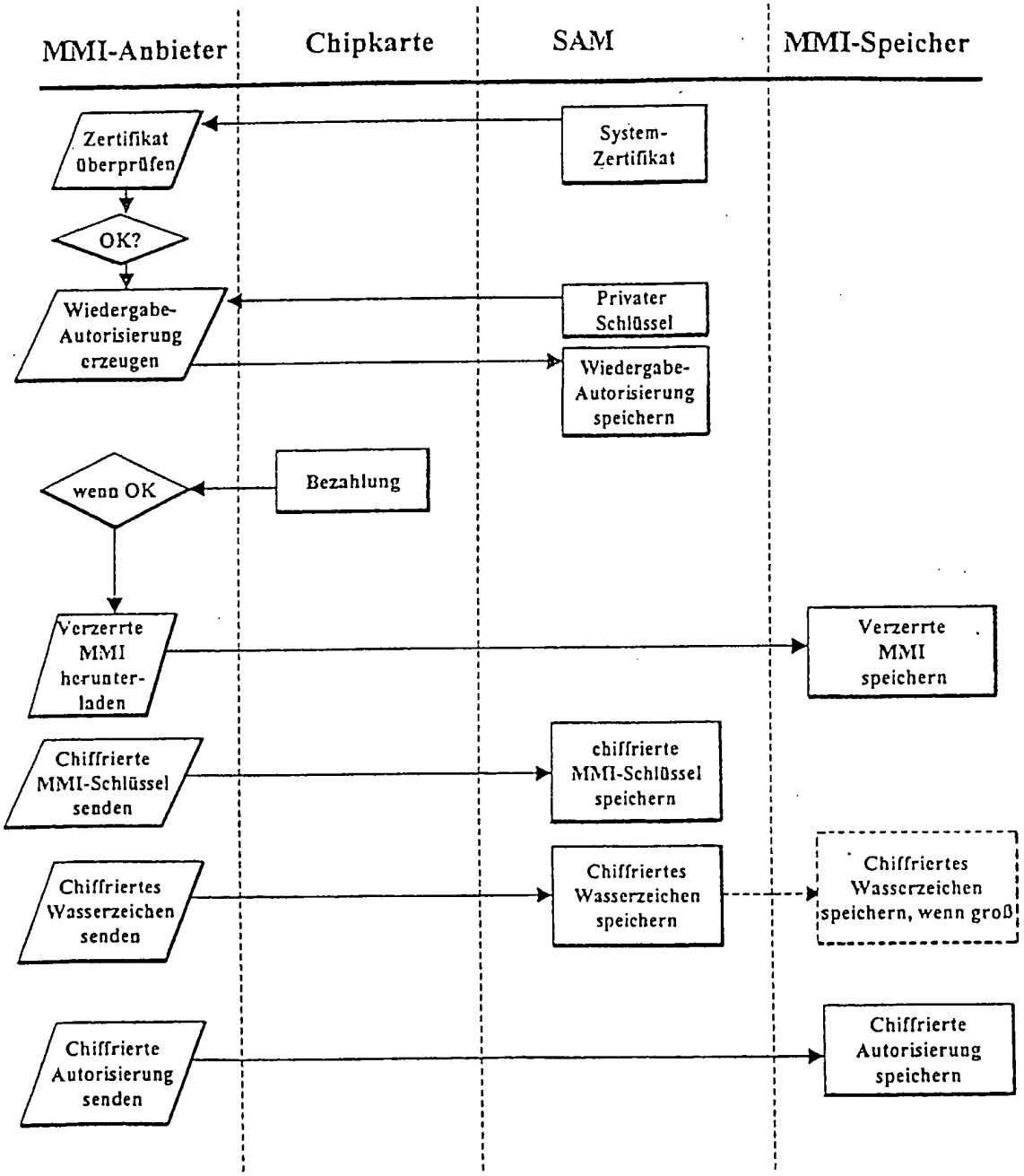


Fig. 3

Überprüfung Wiedergabe-Autorisierung

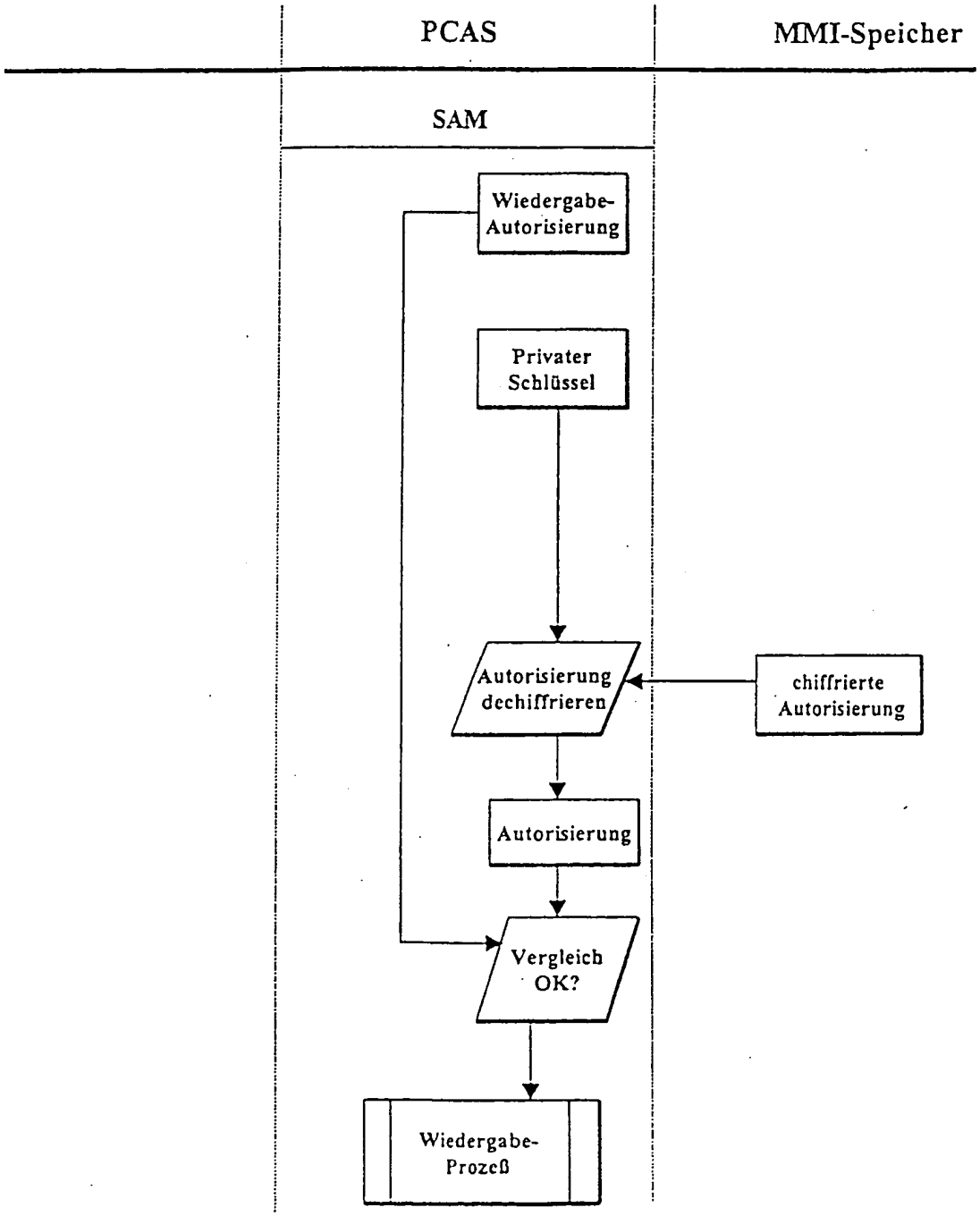
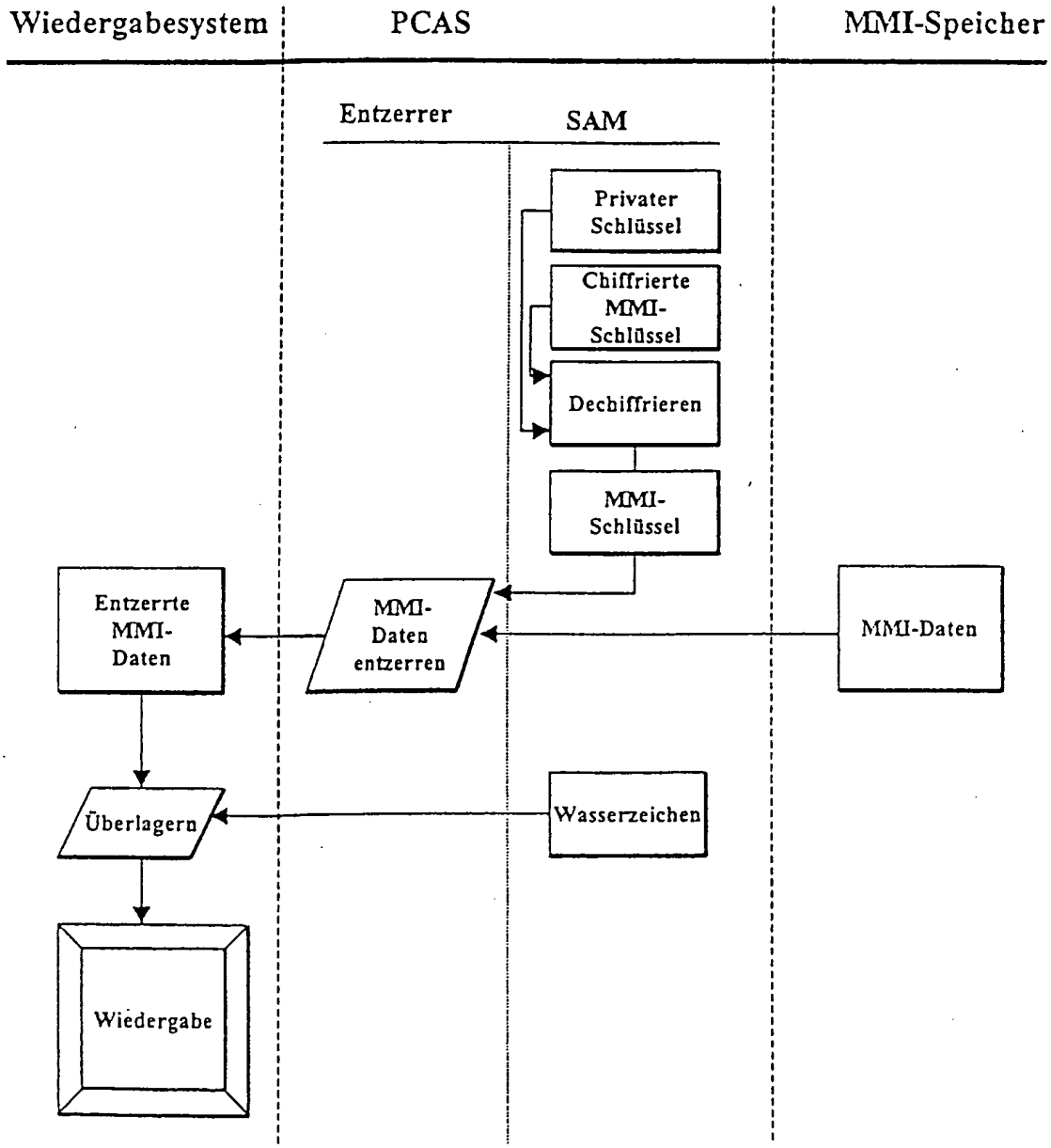


Fig. 4
Wiedergabe-Prozeß



INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/EP 00/02414

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 298 02 270 U (SCM MICROSYSTEMS GMBH) 30 April 1998 (1998-04-30) page 1 -page 17 figures 1-5 ---	1,2, 5-15, 18-20
A	DE 298 05 046 U (SCM MICROSYSTEMS GMBH) 23 July 1998 (1998-07-23) page 1 -page 5 figures 1,2 ---	1,2,6, 8-15, 18-20
A	EP 0 191 162 A (IBM) 20 August 1986 (1986-08-20) abstract column 6, line 8 -column 11, line 16 --- -/--	1-3,6, 10-18, 20,21

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 August 2000	22/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jacobs, P

Form PCT/ISA/210 (second sheet) (July 1992)

2/26/07, EAST Version: 2.1.0.14

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 00/02414

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category ³	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 302 710 A (IBM) 8 February 1989 (1989-02-08) abstract page 2 -page 5 ---	1,3,6, 8-12,16, 18
A	WO 96 35987 A (MACROVISION CORP) 14 November 1996 (1996-11-14) page 9 -page 14, line 2 ---	1,6, 8-13,18, 20
A	EP 0 844 550 A (AT & T CORP) 27 May 1998 (1998-05-27) -----	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

2/26/07, EAST Version: 2.1.0.14

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter nal Application No
PCT/EP 00/02414

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 29802270 U	30-04-1998	WO 9941909 A	19-08-1999
DE 29805046 U	23-07-1998	WO 9948284 A	23-09-1999
EP 0191162 A	20-08-1986	CA 1238427 A	21-06-1988
		DE 3587072 A	18-03-1993
		DE 3587072 T	12-08-1993
		JP 1630801 C	26-12-1991
		JP 2060007 B	14-12-1990
		JP 61145642 A	03-07-1986
		US 4757534 A	12-07-1988
EP 0302710 A	08-02-1989	US 4866769 A	12-09-1989
		CA 1292791 A	03-12-1991
		JP 1044542 A	16-02-1989
WO 9635987 A	14-11-1996	AU 702649 B	25-02-1999
		AU 6029896 A	29-11-1996
		BG 101999 A	31-07-1998
		BR 9609249 A	18-05-1999
		CA 2218383 A	14-11-1996
		CN 1185217 A	17-06-1998
		EP 0879533 A	25-11-1998
		JP 11505658 T	21-05-1999
		NZ 309989 A	29-03-1999
		PL 325440 A	20-07-1998
		US 5754648 A	19-05-1998
		US 5754649 A	19-05-1998
EP 0844550 A	27-05-1998	US 6005935 A	21-12-1999
		JP 10240520 A	11-09-1998

2/26/07, EAST Version: 2.1.0.14

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/02414

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00 G11B20/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F G11B G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 298 02 270 U (SCM MICROSYSTEMS GMBH) 30. April 1998 (1998-04-30) Seite 1 -Seite 17 Abbildungen 1-5 ---	1,2, 5-15, 18-20
A	DE 298 05 046 U (SCM MICROSYSTEMS GMBH) 23. Juli 1998 (1998-07-23) Seite 1 -Seite 5 Abbildungen 1,2 ---	1,2,6, 8-15, 18-20
A	EP 0 191 162 A (IBM) 20. August 1986 (1986-08-20) Zusammenfassung Spalte 6, Zeile 8 -Spalte 11, Zeile 16 --- -/--	1-3,6, 10-18, 20,21

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
14. August 2000	22/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jacobs, P

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

2/26/07, EAST Version: 2.1.0.14

INTERNATIONALER RECHERCHENBERICHT

Inte. .onales Aktenzeichen
PCT/EP 00/02414

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 302 710 A (IBM) 8. Februar 1989 (1989-02-08) Zusammenfassung Seite 2 -Seite 5 ---	1,3,6, 8-12,16, 18
A	WO 96 35987 A (MACROVISION CORP) 14. November 1996 (1996-11-14) Seite 9 -Seite 14, Zeile 2 ---	1,6, 8-13,18, 20
A	EP 0 844 550 A (AT & T CORP) 27. Mai 1998 (1998-05-27) -----	

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

2/26/07, EAST Version: 2.1.0.14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inten .nales Aktenzeichen
PCT/EP 00/02414

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 29802270 U	30-04-1998	WO 9941909 A	19-08-1999
DE 29805046 U	23-07-1998	WO 9948284 A	23-09-1999
EP 0191162 A	20-08-1986	CA 1238427 A	21-06-1988
		DE 3587072 A	18-03-1993
		DE 3587072 T	12-08-1993
		JP 1630801 C	26-12-1991
		JP 2060007 B	14-12-1990
		JP 61145642 A	03-07-1986
		US 4757534 A	12-07-1988
EP 0302710 A	08-02-1989	US 4866769 A	12-09-1989
		CA 1292791 A	03-12-1991
		JP 1044542 A	16-02-1989
WO 9635987 A	14-11-1996	AU 702649 B	25-02-1999
		AU 6029896 A	29-11-1996
		BG 101999 A	31-07-1998
		BR 9609249 A	18-05-1999
		CA 2218383 A	14-11-1996
		CN 1185217 A	17-06-1998
		EP 0879533 A	25-11-1998
		JP 11505658 T	21-05-1999
		NZ 309989 A	29-03-1999
		PL 325440 A	20-07-1998
		US 5754648 A	19-05-1998
		US 5754649 A	19-05-1998
EP 0844550 A	27-05-1998	US 6005935 A	21-12-1999
		JP 10240520 A	11-09-1998

2/26/07, EAST Version: 2.1.0.14